A Pseudo Random Number Generator Based on 4D Hyperchaotic Systems, Riddled Basins of Attraction and Advanced Microfluidic Technology

Nawres A. Alwan[1], Suzan J. Obaiys[1(✉)], Nadia M. G. Al-Saidi[2], Nurul Fazmidar Binti Mohd Noor[1], and Yeliz Karaca[3,4]

[1] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
s2000740@siswa.um.edu.my, {suzan,fazmidar}@um.edu.my
[2] Department of Applied Sciences, University of Technology, Baghdad, Iraq
nadia.m.ghanim@uotechnology.edu.iq
[3] University of Massachusetts (UMass) Chan Medical School, 55 Lake Avenue North, Worcester, MA 01655, USA
yeliz.karaca@ieee.org
[4] Massachusetts Institute of Technology (MIT), 77 Massachusetts Avenue, Cambridge, MA 02139, USA

Abstract. A pseudo random number generator (PRNG), also referred to as a deterministic random bit generator (DRGB) is an algorithm utilized to generate a sequence of numbers which have approximate properties pertaining to those of sequences in random numbers. The current PRNGs can be exemplified as linear congruence generators, inverse congruence generators as well as PRNGs that are based on chaotic systems which have benefits like pseudorandom behavior, sensitivity to initial conditions, ergodicity and high complexity. Accordingly, this paper presents a new mode of PRNG sequences by combining microfluidic (MF) techniques with hyper-chaotic systems of n-dimension. The proposed system offers complex behavior, wide distribution, and plausible ergodicity. This interdisciplinary technique combines engineering, physics, and mathematics to create a random sequence. The mixture of the four outcome sequences generated from the 4 dimensions (4D) hyperchaotic system and the Fisher-Yates Shuffle algorithm is used to generate the PRNG. The algorithmic process is designed to rearrange the sequence elements in a random order. Statistical analysis of the NIST test, key sensitivity, auto-correlation and cross-correlation, and entropy are also presented that play a significant role in demonstrating the PRNG methods.

Keywords: Hyperchaotic · Chaos · Pseudo Random Number Generator (PRNG) · Randomness analysis · Microfluidic · Auto-correlation and cross-correlation tests · Entropy · Permutation entropy · Fisher-Yates Shuffle algorithm · Riddled basins of attraction · Chaotic systems · Fixed point analysis · Conservation system · Bifurcation diagrams of systems

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14815, pp. 91–109, 2024.
https://doi.org/10.1007/978-3-031-65154-0_6

1 Introduction

Pseudo-random number generators (PRNG) are widely utilized across various disciplines such as statistics, computer science, cryptography, and gaming [1]. These generators produce random number series that are derived from a specific starting point through a mathematical formula. In the field of cryptography, the efficacy of PRNG is crucial due to the security process of cryptosystems relies on the randomness and unpredictability of the key generations. A high-quality PRNG must embody some essential attributes to guarantee the security and integrity of the outputs, such as; stochasticity, erraticism, periodicity, security, and efficiency [3]. Typically, PRNGs can be classified into two categories: linear and nonlinear. Linear PRNGs utilize methods such as linear congruential generators (LCGs) and linear feedback shift registers (LFSRs) to produce pseudorandom sequences [4]. However, these methods have limitations, including shorter periods and reduced randomness. Further, the nonlinear PRNG employs nonlinear transition functions or output functions to convert a linear system to nonlinear ones. This approach is increasingly preferred in cryptography due to its superior randomness [5]. Chaotic nonlinear systems are known for several distinctive features including ergodicity, initial condition to sensitivity, seemingly random actions, and a wide spectrum of behaviors [6]. Since Lorenz discovered chaos in 1963, there has been significant research on chaos and the hyper-chaos phenomena. In 1982, Oishi et al. [7] introduced the first pseudorandom sequence generator using a chaotic system. Then, Liu et al. [8] employed a chaotic system for a binary pseudorandom sequence generation. These efforts incorporated a single chaotic system into the PRNG design. Subsequently, many scholars have proposed various algorithms for designing new PRNGs [9–14]. To improve the unpredictability of the sequences created, several security measures were put in place, demonstrating the capability of the generator to produce secure pseudo-random number sequences (PRNS). In 2021, Yu et al. [12] introduced a PRNG based on a chaotic system with an enhanced Hopfield neural network, aimed at reducing chaotic degradation's effects and improving PRNS quality. In 2022, Zang and team [14] proposed a method for PRNS generation based on complex polynomial chaotic maps, exhibiting strong randomness in the PRNS and susceptibility to differential attacks. A notable drawback of chaos-based cryptographic methods is their reliance on chaotic maps that operate with real numbers, which are not ideal for finite numbers cryptographic uses. The quantization of real numbers to round-off values can lead to issues, including the creation of non-reversible functions, thus rendering decryption unfeasible. In 2023, Li et al. published a new PRNG based on a 4D discrete system that has been developed to address issues found in previous literature, including a focus on continuous or low-dimensional chaotic systems characterized by strong temporal correlations and a lack of complex nonlinear dynamics [15]. Haider et al. [16] introduced a novel PRNG based on multivariable optimization for image-cryptographic algorithms. While Shunsuke et al. [17] presented a novel design of random number generators based on chaos-based extremum coding. The security flaws of PRNGs established in linear systems are primarily due to their brief cycle lengths. This shortcoming is exacerbated by the rapid deterioration seen in low-dimensional chaotic systems, which further diminishes the period and randomness of PRNG constructions. The simultaneous presence of chaotic attractors and periodic points in conservative hyper-chaotic systems makes them

less suitable for pseudo-random number generator (PRNG) design due to inherent predictability and difficulty in control [16]. Instead, attention has shifted towards dissipative hyper-chaotic systems within the nonlinear system-based PRNGs era. The robustness of PRNGs derived from these systems hinges on their complexity and the extent of chaotic breakdown. Chaotic systems that exhibit complex dynamic behaviors are known for their enhanced randomness [5]. One of the most critical measures of this randomness is the Lyapunov exponent (LE), with the maximum LE being particularly indicative of the system sensitivity to initial conditions, the higher the exponent the more rapidly trajectories diverge, indicating greater system sensitivity. The weakness of conventional PRNG methodologies, attributed to the simplistic nature of chaotic systems, is evidenced by phenomena such as discontinuous chaotic domains, constricted chaos boundaries, and suboptimal obfuscation and diffusion capabilities [18–20]. Hence, the inception of a novel PRNG approach, characterized by enhanced complexity and stochastic properties, is advocated. Consequently, this paper introduces a new hyperchaotic system, inspired by prior investigations and conceptualizations, demonstrating significantly augmented dynamic complexity. This newly devised chaotic system manifests across a broad continuum of parameters sans periodic windows, exhibiting heightened sensitivity to infinitesimal variances in initial conditions and displaying intricate dynamic behaviors with hyperchaotic attributes, thereby ensuring robust ergodicity. By considering these characteristics, they are considered important for many applications (e.g., image encryption [6]).

Herein, a new PRNG technique commences from the random sequences (SQ) emanating from the newly developed hyperchaotic system of microfluidic (MF) properties is presented. This technique distinguishes itself by utilizing a dynamic MF, engendered from the hyperchaotic scheme. Then, we use the FYS algorithm [21] to shuffle the SQ and randomly distribute its elements to produce the new PRNG is sequence. The converted 32-bit binary representation SQ outcome from the last 16 bits is extracted and presented in a decimal number. This decimal number is then subjected to a modulo 256 operation, aligning the output with the requirements of cryptographic applications and simulations necessitating high-quality randomness. The performance of the proposed mode is evaluated using statistical analysis of the NIST test, key sensitivity, auto-correlation & cross-correlation, and Entropy.

The literature review conducted reveals that numerous PRNG techniques, which utilize one or more chaotic maps, have been introduced. However, there is a notable redundancy in the application of these maps and their combinations. This sort of negligence compromises the PRNG security and robustness. Accordingly, the key contributions of this work include the following aspects: 1) A new 4D hyperchaotic system is developed. 2) Verification of the proposed system's effectiveness through passing all dynamical analyses is ensured. 3) A new method to generate PRNG that employs the 4D hyperchaotic system and Microfluidic technical is provided. 4) Verification of the proposed method is effectiveness through passing all tests in the NIST SP 800 analysis suite is presented.

The paper is structured as follows: Sect. 2 describes the proposed dynamical system and analysis of it. Afterwards, Sect. 3 provides the details of the proposed PRNG

methodology. Section 4 evaluates the performance and discusses the results obtained from the various analyses. Finally, Sect. 5 concludes the paper.

2 Proposed Dynamical System

This section presents the new 4D- hyperchaotic system which is designed for random SQ generation. The 4D-hyperchaotic system can be described as follows:

$$\begin{aligned} \frac{dx_1}{dt} &= (\beta x_2 - \gamma x_3)\, x_4; \quad \frac{dx_2}{dt} = (\gamma x_3 - \delta x_4)\, x_1; \frac{dx_3}{dt} = (\delta x_4 - \alpha x_1)\, x_2; \\ \frac{dx_4}{dt} &= (\alpha x_1 - \beta x_2)\, x_3; \end{aligned} \tag{1}$$

where x_1, x_2, x_3 and x_4 are initial state, and α, β, γ, and δ are parameters. The electrical circuit corresponding to system 1 is depicted in Fig. 1(a), indicating its real-life applicability. Figure 1(b) shows the phase spaces of system 1 for x_1 vs. x_2 using the electrical circuit shown in Fig. 1 of x_1 vs. x_2.

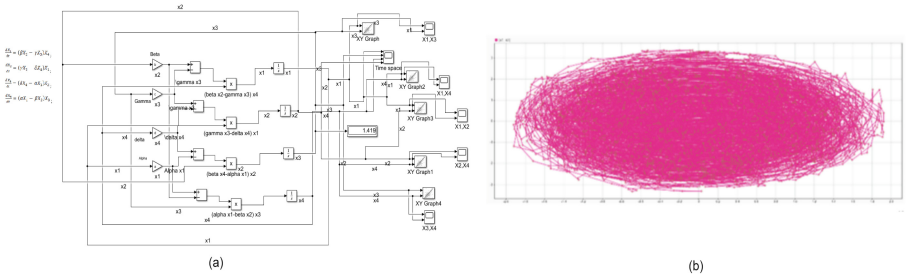

Fig. 1. System 1 (a) circuit using MATLAB Simulink, (b) The phase space of system 1 using MATLAB Simulink of x_1 vs. x_2.

2.1 The Attractor

System 1 attractor is described as a collection of points or a sequence of values within the state space, illustrating the trajectory followed by the system's output. Figure 2(a)–(b) displays the attractor diagrams and time series for the 4D-hyperchaotic system, which are generated under varying parameter values of $\alpha, \beta,\ \gamma,\ \delta$ to $60, 40, 8, 20$ and an initial state of (x_1, x_2, x_3, x_4) to $(1, 1, 2, 2)$. This visualization captures the dynamic behavior and the complexity of the system's evolution over time based on these specific settings. Figure 2(c) shows the sensitivity of the attractor diagrams of the system 1 based on different values of the parameters $(\alpha, \beta,\ \gamma,\ \delta)$ and initial state $(x_1,\ x_2,\ x_3,\ x_4\ )$, where parameters are fixed $\alpha = 40$; $\beta = 60$; $\gamma = 8$; and the value of δ is change into

three values $\delta = 3$, and $\delta = 3.2$ corresponding the attractor diagram with different values of the initial states (x_1, x_2, x_3, x_4)= (1, 1, 2, 2), (1, 1, 2, 2.2), and (1, 1, 2, 2.4) as blue, red, and green, respectively. Analysis of the sensitivity to initial conditions and parameters in any chaotic map reveals a critical dependence on both aspects. Sensitivity to the initial conditions sensitivity demonstrated notable reaction to minimal alterations, with the initial condition x_4 adjusting to merely 0.1 and the parameter δ by 0.2. Subsequent examination and comparison of the resulting trajectories have emphasized this observation.

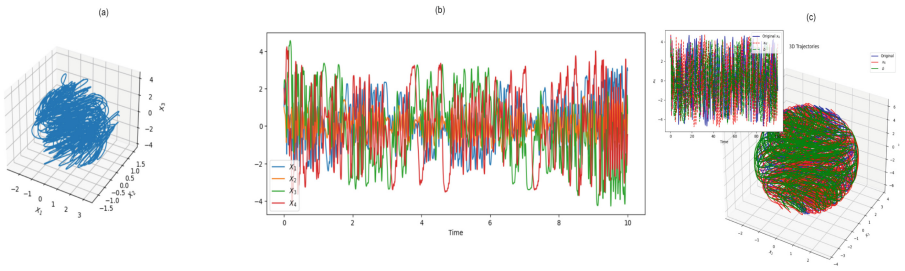

Fig. 2. (a)–(b) Attractors and time series of 4D- hyperchaotic system, respectively, (c) The sensitivity of the system 1 for the Parameters x_4 and b.

Figure 3 shows the phase portraits for pairs of state variables from system 1, (a) x_1 vs. x_2, and (b) x_3 vs. x_4. These plots provide a visual dynamical representation of the system in phase space, illustrating how the state variables interact with each other over the time frame.

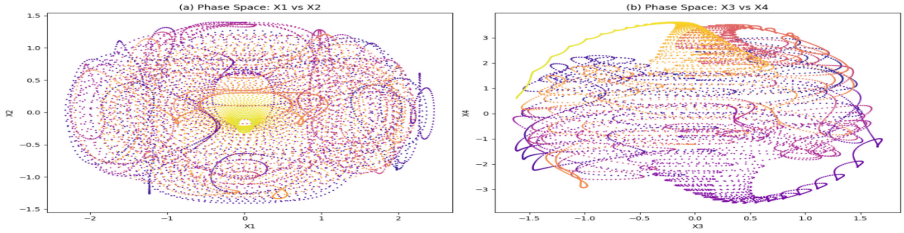

Fig. 3. Phase space of system 1 (a) x_1 vs. x_2, and (b) x_3 vs. x_4.

2.2 Bifurcation Diagram

In the field of dynamic systems, a bifurcation diagram represents a situation in which new behaviors arise when parameters are altered. The diagram serves as a visual representation of the number of possible states that a system can have under various parameter conditions. It uses dots for chaotic behavior and lines for non-chaotic behavior.

Figure 4 (a, b, c, d) depicts the bifurcation diagrams of the system 1 respectively, where $(x(1), x(2), x(3), x(4) = (1, 0.1, 0, 1))$ and various parameters $\alpha \in (60 : 0.01 : 61)$,$\beta \in (40 : 0.01 : 41)$, $\gamma \in (7 : 0.01 : 8)$ and $\delta \in (20 : 0.01 : 21)$.

2.3 Lyapunov Exponent

Lyapunov exponents (LE) serve as a measure for the rate at which trajectories in a system either diverge or converge. These exponents can be mathematically represented as follows [6]:

$$\lambda \approx \frac{1}{t} \ln \frac{||\delta x(t)||}{||\delta x(0)||}$$

Here, the term $\frac{||\delta x(t)||}{||\delta x(0)||}$ denotes the relative distance between two distinct trajectories. Figure 5, depict (a), (b), and (c), the hyperchaotic behavior of a system (1) is illustrated using LE, particularly for the parameter sets $(\alpha = 40; \beta = 60; \gamma = 8; \delta = 20)$, $(\alpha = 40; \beta = 60; \gamma = 8; \delta = 20)$ and $(\alpha = 40; \beta = 60; \gamma = 8; \delta = 20)$, respectively.

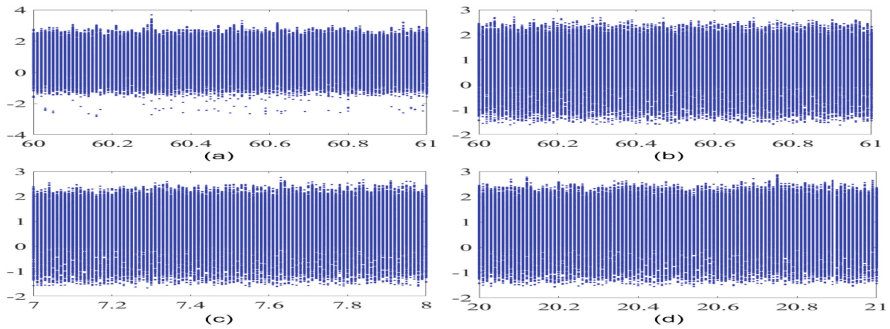

Fig. 4. Bifurcation diagrams of system 1 where the initial state $(x(1), x(2), x(3), x(4) = (1, 0.1, 0, 1))$ and various parameters (a) $\alpha \in (60 : 0.01 : 61)$,(b) $\beta \in (40 : 0.01 : 41)$,(c) $\gamma \in (7 : 0.01 : 8)$, and (d) $\delta \in (20 : 0.01 : 21)$.

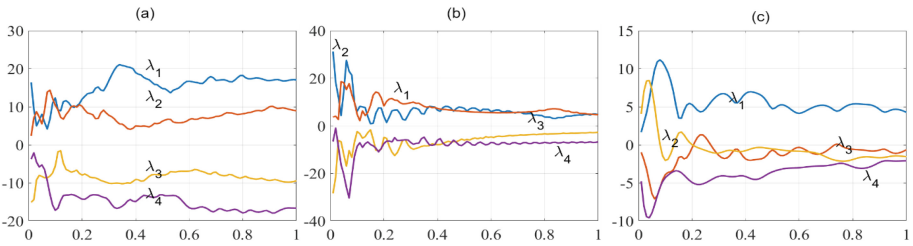

Fig. 5. The Lyapunov exponents of system 1 where the initial state $(x(1), x(2), x(3), x(4) = (1, 0.1, 0, 1))$ and various parameters $(\alpha, \beta, \gamma, \delta)$ (a) $(60, 40, 8, 20)$, (b) $(90, 40, 7, 3)$, and (c) $(60, 30, 3, 10)$.

2.4 Permutation Entropy

Permutation entropy (PE) [22] serves as a crucial measure for assessing the complexity level of time series. It indicates how closely the behavior of chaotic maps mimics pseudo-random sequences. A higher complexity score suggests a closer resemblance to pseudo-random sequences, thereby implying enhanced security. Figure 6 shows the PE for all variables.

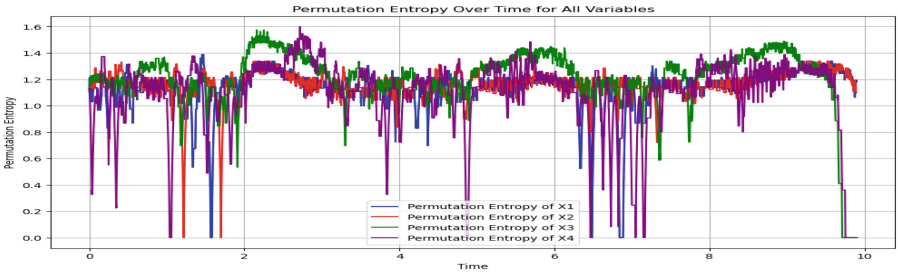

Fig. 6. PE Over Time for All Variables

2.5 Poincaré map

The Poincaré section, also known as the Poincaré map [22], is a crucial tool in the study of dynamical systems, particularly in the analysis of chaotic systems. It provides a way to reduce the dimensionality of a system by taking a cross-section of the phase space, which can simplify the visualization and understanding of the system's dynamics. By studying the intersections of a trajectory with the Poincaré section, one can observe patterns that reveal the underlying structure of the chaotic system. Figure 7(a) shows the simplified Poincaré section of the system 1, focusing on the periodic nature of the dynamics. Two distinct points are shown in red on the section plane, indicating where the system's trajectory intersects the plane in opposite directions. This pattern of intersections suggests a potential periodic orbit within the chaotic system. The semi-transparent grey plane represents the chosen Poincaré section for this analysis, providing a backdrop for the intersection points. In Fig. 7(b), a 2D projection of a Poincaré section is shown for the system 1. The section reveals a series of points where the system's trajectory crosses the section plane, with blue dots indicating the 'in' direction and red dots the 'out' direction of the flow. This differentiation helps to distinguish between the points where the trajectory enters and exits the section plane, respectively. The clustered nature of the points around the central region suggests a looping pattern, characteristic of periodic orbits embedded within the chaotic attractor. Figure 7(c) shows a 2D of the Poincaré section points in and out-direction, where in-direction will be where the sign of x_4 changes from negative to positive, and out-direction will be where the sign changes from positive to negative. Figure 7 (d) illustrates the Poincaré section points with a linear regression line fitted to them. The fitted

line equation is $y = -0.0335x + 0.5136$, with a very low of coefficient of determination R^2 value of 0.0012. The Poincaré section points are shown in blue color, which representing their position in the three-dimensional space. The red plane represents the linear regression fit extended into this space, with the x_1 and x_2 variables.

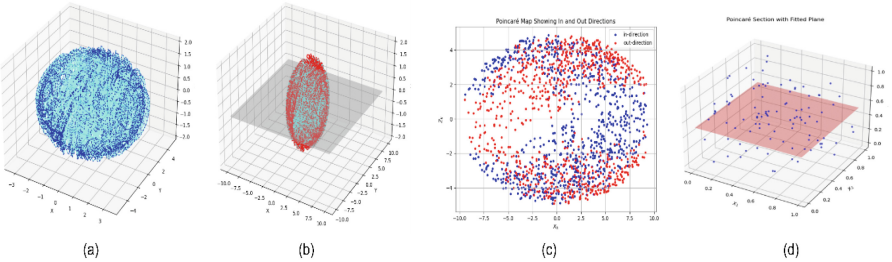

Fig. 7. (a) chaotic flow of system 1 intersecting the Poincaré section, (b) its corresponding Poincaré map, (c) 2D of Poincaré map and (d) Poincaré map

2.6 Conservation and Fixed Points and Basin of Attractor

Conservation: To assess whether the phase space volume of the system exhibits conservative or dissipative characteristics, it is necessary to compute the conservative of the system described in 1. The divergence of the vector field $\mathbb{C}\mathbf{F}$, denoted by $(\nabla \cdot \mathbb{C}\mathbf{F})$ is determined by the aggregate of the partial derivatives associated with each equation in 1, which can be expressed as:

$$\nabla \cdot \mathbb{C}\mathbf{F} = \sum_{i=1}^{4} \frac{\partial}{\partial X_i} (\text{RHS of the } i\text{−th equation})$$

where $\frac{\partial}{\partial X_i}$ is applied to the corresponding right-hand side of the i-th differential equation of system 1, which is expanded as.

$$\nabla \cdot \mathbf{CF} = \frac{\partial}{\partial x_1} (\beta x_2 - \gamma x_3)\, x_4 + \frac{\partial}{\partial x_2} (\gamma x_3 - \delta x_4)\, x_1 + \frac{\partial}{\partial x_3} (\delta x_4 - \alpha x_1)\, x_2 + \frac{\partial}{\partial x_4} (\alpha x_1 - \beta x_2)\, x_3 \tag{2}$$

It is obvious that the first term $\frac{\partial}{\partial x_1} (\beta x_2 - \gamma x_3)\, x_4 = 0$, and the second term $\frac{\partial}{\partial x_2} (\gamma x_3 - \delta x_4)\, x_1 = 0$, since x_1 and x_2 do not appear in the expansion, and so on for the other terms. Then we have;

$$\nabla \cdot \mathbb{C}\mathbf{F} = 0 + 0 + 0 + 0 = 0.$$

Since the $\nabla \cdot \mathbb{C}\mathbf{F} = 0$, this indicates that system 1 holds to conservation laws, indicative of Hamiltonian or conservative systems. According to Liouville's theorem [23], such a condition ensures that the phase space density, along with the system's trajectories, remains constant over time. This indicates that the volume of the phase space is invariant under the system's dynamics, marking a significant contrast to dissipative systems, in which the phase space volume typically decreases over time. Therefore, a system meeting the condition $\nabla \cdot \mathbb{C}\mathbf{F} = 0$ is classified as a conservative dynamical system, characterized by the conservation of energy or analogous quantities, devoid of dissipative effects.

Fixed Points: To determine the equilibrium points, we set the derivatives of all variables to zero. Therefore, applying $\frac{dx_i}{dt} = 0; i = 1, 2, 3, 4$, we get the following equations:

$$(\alpha x_2 - \gamma x_3)\, x_4 = 0; \quad (\beta x_3 - \delta x_4)\, x_1 = 0; (\gamma x_4 - \alpha x_1)\, x_2 = 0; \quad (\delta x_1 - \beta x_2)\, x_3 = 0;$$

This implies that one set of equilibrium points is $x_1 = x_2 = x_3 = x_4 = 0$, while $x_1 = \frac{\beta x_2}{\delta}; x_2 = \frac{\beta x_3}{\alpha}; x_3 = \frac{\gamma x_4}{\beta}; x_4 = \frac{\alpha x_1}{\gamma}$. Figure 8(a) shows the equilibrium points (E_1, E_2) and trajectory of system 1, where the parameter sets $(\alpha = 40; \beta = 60; \gamma = 8; \delta = 20)$ and initial state sets $(x_1 = 1; x_2 = 1; x_3 = 1; x_4 = 1)$.

Basins of Attraction: Riddled basins of attraction represent a complex structure within the phase space of multistable chaotic systems, where the regions of convergence towards different attractors intricately intermingle. This intricate pattern signifies that infinitesimally close initial conditions can result in divergent long-term behaviors, leading to unpredictable transitions between attractors. The presence of riddled basins underscores the sensitivity of the system's ultimate state to its initial conditions, a hallmark of chaotic dynamics. Such behavior has profound implications for predicting the long-term behavior of physical, biological, and engineering systems, as it highlights the limitations posed by inherent unpredictability [24]. Figure 8(b) shows the riddled basins of attraction for a dynamical system. Where the different colors in the plot represent different basins of attraction. The basins of different attractors are intricately interwoven, such that a very small change in initial conditions represented by the x_1 and x_2 axes can lead to convergence to a different attractor. This characteristic makes predicting the long-term behavior of the system quite challenging and is a hallmark of chaotic systems with sensitive dependence on initial conditions.

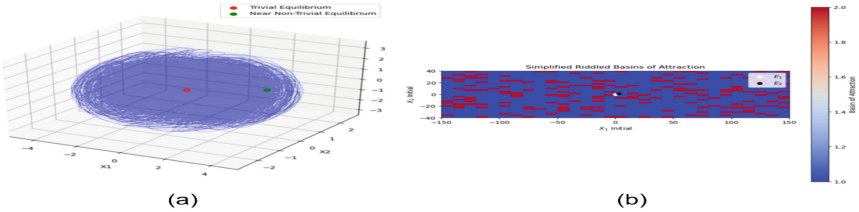

Fig. 8. (a) Equilibrium points and attractor trajectory and (b) Riddled basins of attraction in $x_1(0)$ – $x_2(0)$, and the equilibrium points E_1 and E_2.

3 Proposed Method

3.1 Microfluidic Technology

Microfluidics (MF)refers to a system that manipulates a little amount of fluid by the use of small canals in a specific dimension, and based on this, microfluidic technology is stated to be potentially employed as a platform for the investigation of interactions between drug carriers and cells as well as the treatment implications of active compounds and drugs. Thus, it provides the possibility of analyzing the response of multiple cells, tissues or organs, which can pave the way for the development of novel treatments. MF is one of the important field of science, particularly in, chemical analysis, biological research, diagnostics and the development of new materials [25]. MF deals with the processing of fluids on a very small scale, typically in channels with dimensions ranging from tens to hundreds of micrometers. The principal work of MF is on controlling the behavior, manipulation, and analysis of very small volumes of fluids. Moreover, it enhances some physical properties such as laminar flow, surface tension, fluidic resistance and others. MF technology allows for the miniaturization of laboratory processes, reducing the need for large volumes of reagents and samples, speeding up experiments, and enabling high-throughput testing and analysis with increased efficiency and lower costs, in many scientific areas such as genomics, proteomics, drug discovery and environmental monitoring [25]. Based on this technology, we suggest using this MF technology to mix multiple sequences of random numbers derived from a chaotic dynamical system Instead of fluids, like those in MF. Here are some techniques inspired by MF mixing methods that could be applied to mix random sequences: such as; Serial Dilution, Droplet-Based mixing, Split-and-Recombine (SAR) method, and Fisher-Yates Shuffle algorithm [21].

3.2 Fisher-Yates Shuffle Algorithm

In the technique proposed in this study, we used the Fisher-Yates Shuffle (FYS) algorithm also known as the Knuth shuffle, which is used in MF to mixture the fluids. FYS is an algorithmic process designed to rearrange the elements of the sequence in a random order, which is considered one of the most important methods of shuffling. The FYS algorithm stands as a cornerstone in the domain of random permutations, this is due to

its strong mathematical basis and optimal efficiency in generating uniformly distributed sequences. FYS mathematically can be explained as follows, suppose a sequence S with length n, the first step of the process is starting from the last element and proceeding to the second element in the sequence. At each iteration i, generates random index j is chosen where $1 \leq j \leq i$ and the elements at positions i and j are swapped. Such that, this operation guarantees that each permutation of the sequence has the same probability, establishing the uniform randomness of the algorithm's output. The swap operation is an essential component of the FYS, and involves exchanging the values of two elements within the sequence. For elements at positions i and j, the value at i is temporarily stored, the value at j is placed in position i, and the stored value is then moved to position j. This simple yet effective operation is important for the algorithm's ability to randomize a sequence where each element has the same probability without bias. Based on system 1 and the FSY algorithm, we propose a novel algorithm for generating PRNG sequences. The proposed method begins with the generation of initial values derived from a set of parameters of system 1, and key blocks $K_1, K_2, \ldots, K_{15}$, employing a chaotic system to produce a random sequence of values. These sequences are generated based on system 1 denoted as $SQ(i)$ where i ranges from 1 to 4. Subsequently, these sequences are concatenated into a single sequence SQ, to which the FYS is applied to ensure a uniform distribution of the elements. The final step in the algorithm involves processing the shuffled sequence to produce the PRNG sequence. Each number in the random sequence SQ is converted into a 32-bit binary representation, from which the last 16 bits, which leads to requirements for cryptographic applications and simulations that require high-quality randomness. Through this method, we leverage the deterministic chaos of MF-inspired systems and the confirmatory randomness of FYS to generate PRNG sequences. This approach not only ensures the uniformity and unpredictability essential for cryptographic security but also introduces a novel application of chaos theory in the field of encryption security and random number generation (Fig. 9).

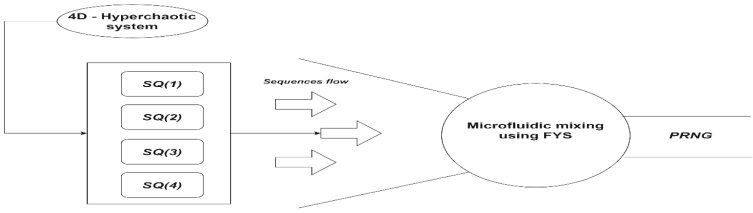

Fig. 9. MF technical to generate PRNG

3.3 Generating Pseudo Random Number Sequences Based on the 4D-Hyperchaotic System in (1)

In this subsection, we discussed the generation of PRNG utilizing systems 1. The initial step involves creating an initial state (x_1, x_2, x_3, x_4) and parameters α, β, γ, and δ of the

system 1. The process for computing new initial values given a set of original initial states and parameters $(x_1, x_2, x_3, x_4, \alpha, \beta, \gamma, \delta)$ along with key blocks $(K_1, K_2, \ldots, K_{15})$. The objective is to produce updated initial values $\left(x_1', x_2', x_3', x_4', \alpha', \beta', \gamma', \delta'\right)$. This is achieved by adjusting each of the original states and parameters by adding the binary-to-decimal conversion of the exclusive or (XOR) operation between specific pairs of key blocks, with a small constant $(1e-6)$ to ensure a minor but significant change. Specifically, $\left(x_1'\right)$ is recalculated by adding (x_1) to the binary-to-decimal conversion of (K_1) XOR (K_2), and similar operations are performed for $\left(x_2'\right), \left(x_3'\right), \left(x_4'\right), (\alpha'), (\beta'), (\gamma')$, and (δ') with their respective key blocks. Such modifications are crucial for boosting the randomness and unpredictability of the initial state (x_0). Algorithm 1 shows the process for generating the initial state (x_0).

Algorithm 1. Generating Initial Values

Input: Original initial states and parameters: $x_1, x_2, x_3, x_4, \alpha, \beta, \gamma, \delta$, Key blocks: $K_1, K_2, \ldots, K_{15}$;
Output: New initial values: $x_1', x_2', x_3', x_4', \alpha', \beta', \gamma', \delta'$;

function $\left[x_1', x_2', x_3' x_4', a', b', c', d'\right]$ = Initial Values $(x_1, x_2, x_3 x_4, \alpha, \beta, \gamma, \delta, K_1, K_2, \ldots, K_{15})$ % Calculate the new initial values

$x_1' = x_1 + \text{bin 2 dec}\,(K_1\ bitxor\ K_2)\ 1e-6;$
$x_2' = x_2 + \text{bin 2 dec}\,(K_3\ bitxor\ K_4)\ 1e-6;$
$x_3' = x_3 + \text{bin 2 dec}\,(K_5\ bitxor\ K_6)\ 1e-6;$
$x_4' = x_4 + \text{bin 2 dec}\,(K_7\ bitxor\ K_8)\ 1e-6;$
$\alpha' = \alpha + \text{bin 2 dec}\,(K_9\ bitxor\ K_2)\ 1e-6;$
$\beta' = \beta + \text{bin 2 dec}\,(K_{10}\ bitxor\ K_{11})\ 1e-6;$
$\gamma' = \gamma + \text{bin2dec}\,(K_{12}\ bitxor\ K_{13})\ 1e-6;$
$\delta' = \delta + \text{bin 2 dec}\,(K_{14}\ bitxor\ K_{15})\ 1e-6;$
Return the new initial values: $x_1', x_2', x_3' x_4', \alpha', \beta', \gamma', \delta'$;

end function

The next stage is the generation of PRNG based on system (1) and MF technique as shown in **Algorithm 4** and Fig. 10, but before that, we introduce some algorithms that should be applied to generate PRNG. In our work, we employed MATLAB 2022b, and we validated the suggested proposed scheme on a personal computer device, powered by CPU 11th Gen Intel(R) Core(TM) i7-11370H @ 3.30GHz 3.30 GHz, and 16.0 GB of RAM.

Where the combine all sequences generated based on system 1 $SQ(1), SQ(2)$, $SQ(3)$, and $SQ(4)$ into a single sequence SQ is a step designed to increase the randomness produced from each iteration, creating a unified sequence that benefits from the complexity and variability inherent in each $SQ(i)$, where $i = 1:4$.

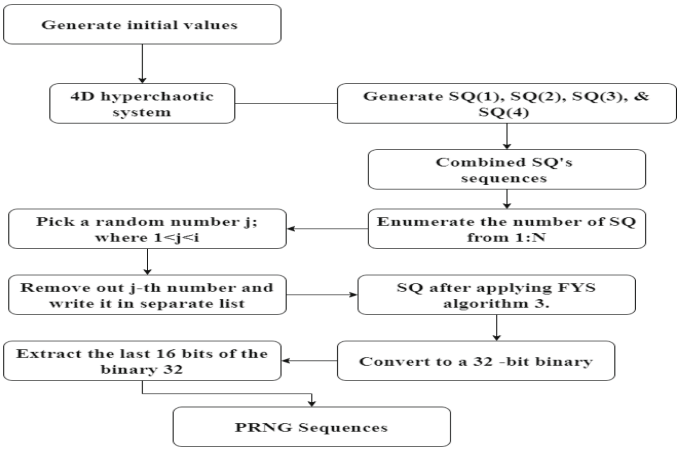

Fig. 10. The PRNG Algorithm

4 Randomness Analysis

4.1 The NIST Test of the System

The National Institute of Standards and Technology (NIST) from the United States offers a standard software package for testing the random behavior of time series.

Algorithm 2. Generation and Combination of Chaotic Sequences

Input: New initial values from Algorithm 1;
Output: Combined sequence SQ

Initialize SQ as empty
for $i = 1 : 4$ **do**
  $\left[x'_1, x'_2, x'_3 x'_4, a', b', c', d'\right]$ = Initial Values $(x_1, x_2, x_3 x_4, \alpha, \beta, \gamma, \delta, K_1, K_2, \ldots, K_{15})$;
  sx_1, sx_2, sx_3, sx_4 % be sequences of equal length n generated from system 1, and let *combined* be the sequence resulting from their zigzag combination.
  combined = [], % an empty sequence;
  for $j = 1, 2, \ldots, n$ **do**% n length of sx_1
    $combined = combined \oplus [sx_1[j]]$
    $combined = combined \oplus [sx_2[j]]$ % Where $\oplus$ denotes the concatenation of elements from each sequence in order.
    $combined = combined \oplus [sx_3[j]]$
    $combined = combined \oplus [sx_4[j]]$
  end for
  $SQ(j) = combined$;
end for
for $i = 1 : 4$ **do**
  $SQ \leftarrow SQ \oplus SQ(i)$% where $\oplus$ denotes the concatenation operation, combining the sequences end-to-end.
end for
return SQ

This package is used to assess the stochastic performance of time series data. The testing process involves evaluating multiple sequences, each consisting of $1,000,000$ bits. NIST employs two key performance metrics, namely the P value and the pass rate, to gauge the randomness of these time series. By default, NIST sets the significance level (α) to 0.01. The pass rate is assessed using a confidence interval formula: $1-\alpha \pm 3\sqrt{\alpha(1-\alpha)/m}$. In this formula, m represents the number of groups of bit sequences. For instance, when α is 0.01 and m is 100, the resulting confidence interval becomes $1\ 0.01 \pm 3\sqrt{0.01 \times 0.99/100} = 0.99 \pm 0.0094393$, which simplifies to the range $[0.9602, 1.0198]$. This implies that the pass rate of the sequence must exceed 0.9602 to meet the required criteria.

We generated a PRNG sequences where the parameters of system 1 are set as $\alpha = 50$, $\beta = 20$, $\gamma = 8$, and $\delta = 20$. A length of 1000000×16 bits binary sequence is obtained, which is divided into 100 groups and each group has a length of 10^6 bits for the NIST test. The outcomes of the experiments are detailed in Table 1. The test results indicate that all P-values exceed 0.01, demonstrating the successful passage of the NIST test by the generated hyperchaotic sequence and comparison with some other works.

Table 1. NIST Statistical test results for the generated hyperchaotic sequences in comparison to some previous methods.

NIST statistical test item	P-value					Results
	Proposed	Ref. [26]	Ref. [16]	Ref. [5]	Ref. [27]	
Block-Frequency	0.3032	0.2028	0.0062	0.5850	0.5852	True
Frequency (Monobit)	0.6240	0.1428	0.6371	0.3939	0.0741	True
Discrete Fourier Transform	0.7721	0.1729	0.9463	0.5456	0.9319	True
Approximate Entropy	0.2352	0.0216	0.0308	0.4444	0.2228	True
Cumulative Sums (Forward)	0.6513	0.2666	0.0757	0.8483	0.0513	True
Cumulative Sums (Reverse)	0.7321	-	0.7399	-	-	True
Serial-1	0.7123	0.3608	0.4373	0.3917	0.3241	True
Serial-2	0.6121	0.4480	0.0329	-	-	True
Runs	0.3312	0.2859	0.1626	0.3504	0.9808	True
Longest Run of Ones	0.7662	0.8303	0.6163	0.8138	0.3781	True
Overlapping Template	0.9717	0.5782	0.0712	0.6066	0.9705	True
Non-overlapping Template	0.3378	0.00001	0.9558	0.6977	0.7727	True
Linear Complexity	0.5341	0.9511	0.1719	0.4091	0.0487	True
Binary Matrix Rank	0.6773	0.8813	0.1296	0.6993	0.2133	True
Maurer's universal statistical	0.4468	0.6342	0.0966	0.4190	0.3371	True
Random Excursions	0.5867	0.7147	0.8195	0.7787	0.4372	True
Random Excursions Variant	0.5778	0.5142	0.8195	0.6815	0.7061	True

4.2 Key Sensitivity Analysis

Key sensitivity analysis evaluates the impact of minor changes in input on the resultant outputs. A system demonstrates high sensitivity if small alterations in the input lead to significant differences in the output. The bit change rate (BCR) is a critical metric for gauging the sensitivity of a system, such as a PRNG, to its initial settings. This concept quantifies the extent of variation between outputs generated from the original and slightly modified inputs. In this study, the initial parameter δ of the hyperchaotic system is increased by 0.1. The PRNG output based on this initial setting is then compared with the output derived from the adjusted value. The BCR evaluating the sensitivity of a PRNG to its initial conditions, measures the proportion of bytes that change between two sequences generated with slightly different initial inputs. This analysis is crucial for assessing the sensitivity of cryptographic systems, where high sensitivity to initial conditions is often desirable for security reasons. The formula for calculating the (BCR) can be defined as:

$$BCR = \left(\frac{\text{Number of differing bytes}}{\text{Total number of bytes}} \right) \times 100\%$$

In our experiment, the (BCR) stands at 99.50% which highlights the system's high sensitivity to initial conditions. Figure 11 shows the key sensitivity analysis of two PRNG sequences, where the PRNG sequence 1 with $\delta = 20$, and sequence 2 with $\delta = 20.1$, which means any tiny change in system 1 leads to the generation of a new PRNG.

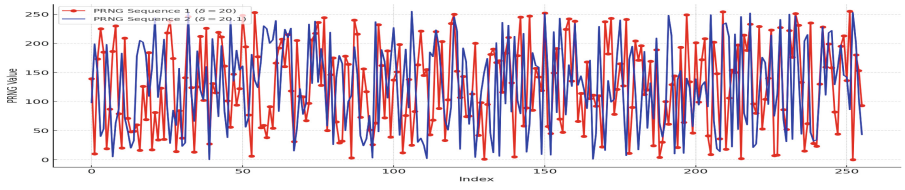

Fig. 11. Key sensitivity analysis of two PRNG sequences.

4.3 Auto-correlation and Cross-correlation

Auto-correlation and cross-correlation tests are statistical tools used to analyze sequences for patterns and relationships. Auto-correlation tests the similarity between a sequence $\{S_i\}_{i=1}^{N}$ and its shifted counterpart $\{S_i\}_{i=j}^{N+j}$, where j ranges from 0 to $N-1$. The auto-correlation at lag k for a sequence S of length N is calculated as:

$$R_s(k) = \frac{1}{(N-k)\sigma^2} \sum_{i=1}^{N-k} (s_i - \mu)(s_{i+k} - \mu)$$

where μ is the mean of x and σ^2 is its variance.

similarly, Cross-correlation, assesses the similarity between two distinct sequences. Employing the same formula, it allows for the comparison of different sequences generated by the scheme in question. The cross-correlation at lag k between sequences S_1 and S_2 of equal length N is:

$$R_{S_1S_2}(k) = \frac{1}{(N-k)\sigma_{S_1}\sigma_{S_2}} \sum_{i=1}^{N-k} (S_{1_i} - \mu_{s_1})(S_{2i+k} - \mu_{S_2})$$

where μ_{S_1} and μ_{S_1} are the means of S_1 and S_2, and σ_{S_1} and σ_{S_2} are their standard deviations.

In this study, both auto-correlation and cross-correlation of sequences produced by the proposed method are examined to assess their similarity and randomness characteristics. Figure 12 shows the auto-correlation and cross-correlation of two PRNG sequences with a length sequence off 200 bits.

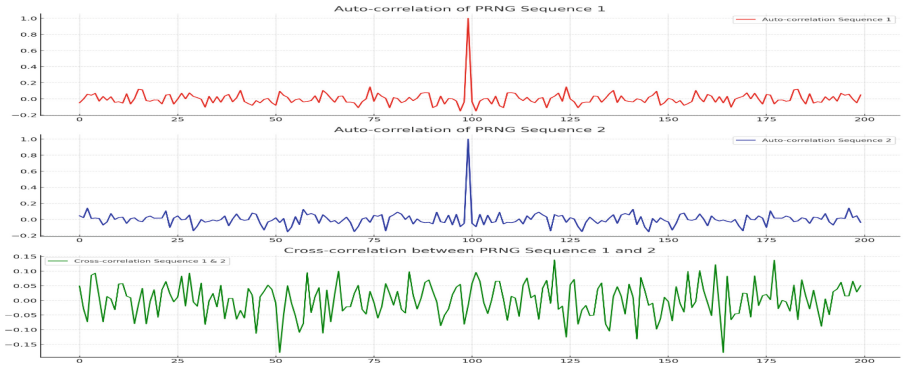

Fig. 12. The auto-correlation test and cross-correlation test of PRNG sequences 1 and 2.

4.4 Entropy

Information entropy is a measure of the unpredictability or randomness of a data source. For a discrete random variable S with possible values $\{s_1, s_2, \ldots, s_n\}$ and probability mass function $P(S = s_i) = p_i$, the entropy $Entropy(S)$ is defined as:

$$Entropy(S) = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

For PRNG sequences, we are interested in the entropy of the distribution of their values. Higher entropy indicates greater randomness and the values of $Entropy(S)$ must be between 1 to 8 indicating a significant level of randomness in both sequences. The closer the $Entropy(S)$ value is to 8, the higher the randomness and unpredictability

of the sequence. To obtain the $Entropy(S)$ of PRNG Sequences, we will first need to estimate the probability distribution of their values. One common approach is to use histogram bins to approximate these probabilities. Table 2 shows the entropy values of our scheme and some other methods, the comparison is based on entropy analysis.

Table 2. Entropy and comparison with other methods.

Scheme	Proposed	Ref. [5]	Ref. [11]	Ref. [28]	Ref. [29]	Ref. [30]	Ref. [31]
Entropy Value	7.975	7.9896	7.9980	7.9985	7.9864	7.9937	7.9692

5 Conclusion and Future Directions

Microfluidics (MF) is a system directing a little amount of fluid through small canals in the dimension ranging from tens to hundreds of micrometers. Based on microfluidics, microfluidic technology can serve as an effective platform to investigate interactions between drug carriers and cells as well as the treatment implications of active compounds and drugs. In addition, a pseudo random number generator (PRNG), which is also known as a deterministic random bit generator (DRGB) is an algorithm which can employed for the generation of a sequence of numbers with approximate properties pertaining to the sequences in random numbers. Accordingly, this paper presents a new mode of PRNG sequences by combining microfluidic (MF) techniques with hyperchaotic systems of n-dimension. Hence, a novel PRNG is proposed based on an MF, and chaotic system. A PRNG algorithm based on a hyperchaotic system is used for this purpose. It uses two main steps, the first of which is generating a hyperchaotic system, and the second step is mixing the SQ used FYS algorithm of MF. The PRNG approach demonstrated outstanding performance through simulation tests, such as, the NIST test, key sensitivity, auto-correlation and cross- correlation and entropy. Furthermore, the result of the BCR stands at 99.50% highlighting the system's high sensitivity to initial conditions. As future directions, the proposed scheme in this study can be extended and developed in a way to provides the possibility of analyzing the response of multiple cells, tissues or organs, which can pave the way for the development of novel treatments while having extensive application areas in applied sciences, engineering and other related realms.

Acknowledgments. This work was accomplished at the University of Technology, Iraq, and the Faculty of Computer Science and Information Technology, Universiti Malaya, Malaysia and it is funded by the Universiti Malaya RMFI2067-2021 Grant.

References

1. Luby, M.G.: Pseudorandomness and cryptographic applications. Princeton University Press (1996)

2. Menezes, A.J., Van Oorschot, P.C., and Vanstone, S.A.: Handbook of applied cryptography. CRC Press (2018)
3. Knuth, D.E.: Art of computer programming, volume 2: Seminumerical algorithms. Addison-Wesley Professional (2014)
4. L"Ecuyer, P.: Random number generation. Springer (2012)
5. Zhao, Y., Gao, C., Liu, J., Dong, S.: A self-perturbed pseudo-random sequence generator based on hyperchaos. Chaos, Solitons Fractals: X **4**, 100023 (2019)
6. Wazi, M.T., Ali, D.S., Al-Saidi, N.M., Alawn, N.A.: A secure image cryptosystem via multiple chaotic maps. Discrete Math. Algorithms Appl. **14**(04), 2150141 (2022)
7. Oishi, S.i., Inoue, H.: Pseudo-random number generators and chaos. IEICE Trans. (1976-1990) **65**(9), 534–541 (1982)
8. Liu, Z., Tang, J., Yu, J.: An application of chaos: generating binary pseudo-random sequences. In: Editor (Ed.) Book An application of chaos: generating binary pseudo-random sequences (IEEE, 1988, edn.), pp. 1–3
9. Akif, Omar Z., et al.: A new pseudorandom bits generator based on a 2D-chaotic system and diffusion property. Bull. Electr. Eng. Inform. **10**(3), 1580–1588 (2021)
10. Al Maliky, S.S.B.: Multidisciplinary perspectives in cryptology and information security. IGI Global (2014)
11. Ullah, I., Azam, N.A., Hayat, U.: Efficient and secure substitution box and random number generators over Mordell elliptic curves. J. Inf. Secur. Appl. **56**, 102619 (2021)
12. Yu, F., et al.: Design and FPGA implementation of a pseudo-random number generator based on a Hopfield neural network under electromagnetic radiation. Front. Phys. **9**, 690651 (2021)
13. Al-Khedhairi, A., Elsonbaty, A., Elsadany, A.A., Hagras, E.A.: Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves. IEEE Access **8**, 57733–57748 (2020)
14. Natiq, H., Al-Saidi, N.M., Obaiys, S.J., Mahdi, M.N., Farhan, A.K.: Image encryption based on local fractional derivative complex logistic map. Symmetry **14**(9), 2022 (1874)
15. Li, S., et al.: A high throughput pseudo random number generator driven by four dimensional discrete hyper chaotic system. Electron. Lett. **59**(18), el2950 (2023)
16. Haider, T., Blanco, S.A., Hayat, U.: A novel pseudo-random number generator based on multivariable optimization for image-cryptographic applications. Expert Syst. Appl. **240**, 122446 (2024)
17. Araki, S., Wu, J.-H., Yan, J.-J.: A novel design of random number generators using chaos-based extremum coding. IEEE Access **12**, 24039–24047 (2024)
18. Al-Saidi, N.M.G., Younus, D., Natiq, H., Ariffin, M.R.K., Asbullah, M.A., Mahad, Z.: A new hyperchaotic map for a secure communication scheme with an experimental realization. Symmetry **12**(11), 2021 (1881)
19. Liu, L., Wang, J.: A cluster of 1D quadratic chaotic map and its applications in image encryption. Math. Comput. Simul. **204**, 89–114 (2023)
20. Ali, D.S., Alwan, N.A., Al-Saidi, N.M.G.: Image encryption based on highly sensitive chaotic system. In: AIP Conference Proceedings, vol. 2183. No. 1. AIP Publishing (2019)
21. Tabeling, P.: Introduction to Microfluidics Oxford University Press. In: Editor (Ed.) Book Introduction to Microfluidics Oxford University Press (Oxford, England ISBN, 2005, edn.), pp. 978–970
22. Veeman, D., et al.: A new megastable chaotic oscillator with blinking oscillation terms. Complexity **2021**, 1–12 (2021)
23. Goldstein, H., Poole, C., Safko, J.: Classical mechanics. In: Editor (Ed.) Book Classical mechanics' (American Association of Physics Teachers, 2002, edn.), pp. 782–783
24. Chazottes, J.-R., Fernandez, B., Ashwin, P.: Riddled basins and coupled dynamical systems. In: Dynamics of Coupled Map Lattices and of Related Spatially Extended Systems, pp. 181–207 (2005)

25. Whitesides, G.M.: The origins and the future of microfluidics. Nature **442**(7101), 368–373 (2006)
26. Hamza, R.: A novel pseudo random sequence generator for image-cryptographic applications. J. Inf. Secur. Appl. **35**, 119–127 (2017)
27. Chen, X., et al.: Pseudorandom number generator based on three kinds of four-wing memristive hyperchaotic system and its application in image encryption. Complexity **2020**, 1–17 (2020)
28. Shi, Y., Deng, Y.: Hybrid control of digital Baker map with application to pseudo-random number generator. Entropy **23**(5), 578 (2021)
29. Agarwal, S.: Designing a pseudo-random bit generator using generalized cascade fractal function. Chaos Theory Appl. **3**(1), 11–19 (2021)
30. Barani, M.J., Ayubi, P., Valandar, M.Y., Irani, B.Y.: A new Pseudo random number generator based on generalized Newton complex map with dynamic key. J. Inf. Secur. Appl. **53**, 102509 (2020)
31. Wang, L., Cheng, H.: Pseudo-random number generator based on logistic chaotic system. Entropy **21**(10), 960 (2019)